ACN | Alerting and Coordination Network

ACN*Report*

Summer 2004 Vol. III, No. 2

A National Security and Emergency Preparedness (NS/EP) Support Program of the National Communications System

In This Issue

PBX Security: The Key to Network Security

Nathy Thongphok
Senior VoIP Engineer

The Alerting and Coordination Network's (ACN) private branch exchange (PBX) is perhaps the single most important element in the ACN infrastructure architecture. Keeping it secure is critical. Essentially a small phone company in a box, the PBX provides the connectivity that defines ACN operations.

The National Institute of Standards and Technology (NIST), in Special Publication 800-24, outlines five major PBX vulnerabilities: system architecture, hardware, maintenance, database software and user features.

PBX security concerns are unique for two reasons. First and most importantly, the PBX often requires remote vendor maintenance. Accordingly, off-site switch accessibility has to be available to external parties. Secondly, the variety of features offered on PBX systems creates more avenues of approach for potential attackers.

A lack of PBX security opens the door to various problems. Long distance service could be illegitimately utilized (often called theft of service or toll

continued on page 2

ACN Set to Expand

The National Communications System (NCS) expects new industry members to join the Alerting and Coordination Network (ACN) this quarter, representing the first ACN membership expansion since 2001. The original membership of ACN totaled 42, but in the last three years, the telecommunications sector experienced significant mergers and downsizing and ACN membership reflects these influences. Today's membership includes 17 Government and industry partners for a total of 32 ACN sites.

In the three years following the transition, the NCS enhanced various components of the technology, such as upgrading the analog lines to voice over Internet protocol capabilities. The NCS completed the upgrades in 2002 and is now focusing on expanding membership.

continued on page 3

The Questionnaire Results are In!

ACN Members Offer Feedback

What is the level of interest in an Alerting and Coordination Network (ACN) Membership Committee? What about a Users Forum? Could materials be provided to enhance the overall ACN experience? How many members actually read this newsletter? The National Communications System (NCS) is constantly striving to build upon an already outstanding network, and who better to ask for input than the ACN user community itself?

The NCS distributed questionnaires on these topics to all ACN members in early

continued on page 4

***PBX** continued from page 1*

fraud). Privileged data might be disclosed. Caller information might be surreptitiously analyzed without permission, and the details disclosed to unauthorized parties. Denial of service could render the PBX inoperable.

PBX system architecture consists of a central computer processor, several microprocessors, and one or more terminals. Network designers should specify the architecture so that administrators can employ proper defense measures, and configure switch and port settings to ensure safe operation.

The primary concern when it comes to PBX hardware is its vulnerability to potential interception of voice traffic by unauthorized users. The interception methodologies can vary and are dependant largely on the communication channels between the PBX and its operating elements. Digital voice (employed by ACN

PBXs) offers the most protection against line tapping. Specific hardware safety measures include anti-tampering devices, cyclic integrity checks and physical security efforts (secure facilities), all of which the NCS has implemented for ACN.

Maintenance precautions are particularly important to PBX security, as most maintenance procedures lead directly to the internal operation of the equipment. To offset maintenance risks, network administrators restrict physical access to the PBXs, secure maintenance terminals and incorporate multi-method security authentication (login/password and smart card validation used together).

Database software presents a different set of challenges. Loading or updating software puts the system at a heightened state of risk. A crash resulting from voice mail or system shutdown procedures might leave the PBX vulnerable to denial-of-service attacks. Software security countermeasures include use of cryptology-based error detection software and password regeneration tools, crash vulnerability testing and embedded password replacement.

The abundance of user features available on a PBX system provides adversaries multiple channels of attack. Attendant override, call forwarding, conferencing, user tracking, and silent monitoring are just a few of the features that make the equipment a valuable commodity and an attractive target for malicious users. Countermeasures for user feature attacks are vast, but the best defense is to ensure that only critical features are enabled.

ACN security is paramount. The NCS continuously monitors the network's PBXs; in the next newsletter, find out what specific actions NCS takes to maintain PBX security.

Mr. Thongphok is a Senior VoIP Engineer for Arrowhead Global Solutions, under contract to the NCS.

ACN Operational Documents

The National Communications System (NCS) is drafting an updated concept of operations (CONOPS) to provide Alerting and Coordination Network (ACN) members with formal guidance concerning how and when the network is to be used. To date, ACN operations conform to the CONOPS in effect when the National Telecommunications Alliance (NTA) operated the network in the late 1990s. The original document, drafted under the leadership of the NTA, addressed issues that were applicable to analog capabilities. The new CONOPS will incorporate ACN's technology upgrade from analog to voice over Internet protocol.

Along with the CONOPS the NCS is drafting a standard operating procedure as a companion document. Both documents will be available in the third quarter of 2004. The NCS encourages ACN members to provide recommendations for both documents.

Social Engineering:

The Latest Way to Hack

Cary Riddock
Security Consultant

An imposter posing as an authoritative figure convinces a help desk technician to disclose a password. An unauthorized e-mail attachment unleashes a Trojan horse. An unfamiliar coworker professes confusion, flashes a smile, and acquires system access. Any of the preceding scenarios might occur in your office, and they all spell trouble. It seems that hackers now have a way to obtain information that doesn't involve breaking and entering or even physical access to the equipment. It's called "social engineering." In its most basic form, "social engineering" is the "low tech" art of getting information from people without them realizing it. The ultimate goal is gaining protected information or unauthorized system access.

Social engineers can ruin your day any number of ways. They'll make a phone call or send an e-mail under the guise of management or information technology support staff. They'll show up at your office asking innocent questions. They'll be persuasive, manipulative, menacing or charming. They'll even rummage through your dumpster, happily snatching up company phone books, calendars, source code and manuals. While the means might vary, the end result never does: the sensitive information your company has gone great lengths to safeguard gets compromised, and chances are you might never even realize it.

The good news is that a little know-how can easily curtail social engineering. Physical security is a good place to start. Thorough badge inspection of anyone entering the facility should be standard company policy. Sensitive documentation, whether in hard or soft copy, should be physically locked down and never sent out in an e-mail or faxed to a "confused" or "helpless" co-worker. All workstations should be password protected, and terminals should be locked when not in use. Computer passwords need to change periodically. Sensitive documentation should be shredded.

Yet physical security alone is not enough. It's essential to have a solid security training and awareness program. Employees who know the importance and definition of confidential information are more likely to take its protection seriously. Along those same lines, employees trained to recognize telltale signs of social engineering stand a better chance of thwarting it. Impatience, intimidation, refusal to disclose contact information, name-dropping and similar idiosyncrasies should immediately raise a red flag.

You can spend a fortune purchasing security hardware, patches and services designed to protect your network, but the hazards of social engineering can't be abolished by a firewall or virus scan. The best weapon is an educated employee. A bit of situational awareness and intellect allows you to turn the table on social engineering.

Mr. Riddock provides network security consulting services for Arrowhead Global Solutions, under contract to the NCS.

Expansion *continued from page 1*

The NCS recently invited nine company participants in the National Coordinating Center for Telecommunications Information Sharing and Analysis Center to join the ACN network; they were not part of the initial ACN membership under the National Telecommunications Alliance. Of the nine, five (Nextel, McLeodUSA, Intrado, Americom, and Level3) are in varying stages of joining the network.

The mission of the ACN, to provide an emergency communications network to support network restoration and coordination, requires the NCS to periodically evaluate the membership to ensure that key Government and industry partners are connected. The NCS will continue to reevaluate ACN membership to maintain operational readiness.

Current ACN Membership

AT&T

BellSouth

Cincinnati Bell Telephone

Cisco Systems

Federal Communications Commission

Lucent Technologies

MCI

Mount Weather Emergency Operations Center

Nortel Networks

Nuclear Regulatory Commission

Qwest

SBC

Sprint

Tekelec

Telcordia Technologies

VeriSign

Verizon

Questionnaire *continued from page 1*

May, and we heard from nearly 90 percent of ACN members. What did the responses divulge? The findings reveal that 85 percent of all sites staff ACN phones 24x7, 50 percent of members are interested in a potential ACN Membership Committee, and 69 percent would join an ACN Users Forum.

Results also confirm the utility of the newsletter. Nearly half of all members read it entirely, with a total of 96 percent perusing it to some degree. ACN members provided recommendations to enhance the newsletter, including future articles discussing situational implementation, secure communications and testing procedures. There is a consensus that training activities (step-by-step network instruction, real-life scenario exercises and emergency response actions) would make the publication even more useful.

Members contributed suggestions to enhance the program, including involvement in Federal exercises, quick-reference cards, semi-annual training exercises and user policy expectations in the future.

The NCS reviewed the responses thoroughly and is incorporating the suggestions into future plans. ACN continues to improve and the input of valued members is a fundamental part of that growth.

Did You Know?

Just after the famous "Mr. Watson come here ...," Alexander Graham Bell was testing his device over a longer distance. Bell and Watson were upstairs with one device while Charles Williams was using the other device downstairs. Someone yelled for Bell from another room and as he left, he handed the device to Watson, saying "here, hold this"; thus the term "putting someone on hold."

Watson, who got bored easily, started humming "Meet Me in St. Louie, Louie." Williams commented that it was nice to hear music while holding for Bell. This was the first case of music on hold.

- www.telephonetribute.com

ACN Program Management Office

Tel: 1-866-NCS-CALL (1-866-627-2255)
1-703-676-CALL (703-676-2255) DC Metro Area
E-mail: acn@ncs.gov
Web: www.ncs.gov

Important Dates

Monthly Test - 3rd Monday of each month between 10am and 2pm EST.

Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
National Communications System
P.O. Box 4502
Arlington, VA 22204-4502

24/7 Help Desk:
1-877- 441- 9330

Technical Support: Service Management Center (SMC)

ACN Ext: 4357 (HELP)
Tel: 1-877-441-9330 (Toll Free)
E-mail: smc@arrowhead.com